

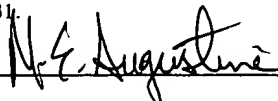
APPLICATION
FOR
UNITED STATES LETTERS PATENT

TITLE: OUT-OF-BAND SIGNALING FOR NETWORK BASED COMPUTER
SESSION SYNCHRONIZATION

APPLICANT: GLENN BEGIS

"EXPRESS MAIL" Mailing Label Number EL253772727US
Date of Deposit April 8, 1999

I hereby certify that this correspondence is being deposited with the
United States Postal Service as "Express Mail Post Office To
Addressee" with sufficient postage on the date indicated above and is
addressed to the Assistant Commissioner for Patents, Washington,
D.C. 20231.



M. E. Augustine

OUT-OF-BAND SIGNALING FOR NETWORK BASED
COMPUTER SESSION SYNCHRONIZATION

5

BACKGROUND

The present disclosure relates to simultaneous use of two separate networks, and the leveraging of connectivity on one network to create a logical connection on the second network.

10 An Internet protocol ("IP") address is used alone, or in conjunction with software endpoints called ports, by applications and communication stacks to establish an Internet connection between two intelligent devices such as computers. The IP address for a computer can be static or
15 assigned dynamically when the computer connects to an intranet or the Internet. A dynamic IP address can change each time the computer connects to an intranet or the Internet.

An IP connection is established after one of the
20 computers discovers the other computer's IP and port addresses before establishing the IP connection. A computer can publish its IP and port addresses in a known location with a known IP address so that another computer can access the first computer's IP and port addresses. These known
25 locations are sometimes referred to as "buddy lists". This

method of establishing an IP connection employs a pre-
arranged agreement to establish the connection.

SUMMARY

5 The present disclosure describes methods and apparatus
for establishing a network connection. In one aspect,
establishing a network connection includes: establishing a
connection across a first communication network that carries
audio signals; encoding a computer network address for a
10 specified network different from the first network into an
encoded network address and sending the encoded network
address across the first network; and using said network
address to establish a network connection on said second
network. In one implementation, network connectivity
15 functionality of a computer can be automatically accessed
using telephone connectivity. Out-of-band signaling
provides a spontaneous network collaboration capability by
sending an Internet protocol ("IP") address across a public
switched telephone network ("PSTN") connection.

20 In another aspect, Internet connectivity provides
privacy across a telephone network through encryption
including: establishing a connection across a voice
communication network between a first party and a second

party; establishing a connection across a computer network between the first party and the second party; transmitting an encryption key across the computer network so that both said first and second parties have said encryption key;
5 encrypting an audio signal using the encryption key; and transmitting the encrypted audio signal across the voice telephone network.

In another aspect, Internet connectivity provides identity authentication of a party to a telephone connection
10 including: establishing a connection across a voice communication network between a calling telephone and a receiving telephone; establishing a connection across a computer network between a calling computer and a receiving computer; and verifying that the calling computer is coupled
15 to the calling telephone by sending a signal from the receiving telephone to the calling telephone across the voice communication network and sending the signal from the calling computer to the receiving computer across the computer network.

20 In another aspect, a crossbar switch provides dynamic allocation of audio input signals and output signals in a computer system and across a network or networks. The crossbar switch includes: a plurality of input ports, where

one input port is coupled to an audio source; a plurality of output ports, where one output port is coupled to a telephone network, and one output port is coupled to a computer network; and a control element which physically
5 connects at least one input port to at least one output port and can dynamically change which input port is coupled to which output port. The switch can be implemented in hardware or software, or a combination of both.

10

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows a block diagram of two computers coupled to respective telephones and interconnected by a computer network and a telephone network.

FIG. 2 is a flowchart of spontaneously establishing an
15 IP connection between users using the PSTN and the configuration shown in FIG. 1.

FIG. 3A is a block diagram showing an audio crossbar switch.

FIG. 3B is a block diagram showing a crossbar switch
20 coupled to a computer.

FIG. 4 is a flowchart of encrypting an audio signal sent over a telephone network, such as the PSTN, using a computer network connection, such as an IP connection.

FIG. 5 is a flowchart of authenticating a caller during a telephone connection across a telephone network, such as the PSTN, using a computer network connection, such as an IP connection.

5 FIG. 6 is a flowchart of verifying the telephone-computer connection between user B's telephone and computer.

DETAILED DESCRIPTION

66040-506860
10 FIG. 1 shows a block diagram 100 of an out-of-band signaling system. A first computer 105 is coupled to a first telephone 110 through a path 107 that allows audio signals and/or data to be exchanged between computer 105 and telephone 110. A second computer 115 is coupled to a second telephone 120 through a path 117 that allows audio signals
15 and data to be exchanged between computer 115 and telephone 120. Computers 105 and 115 can be conventional desktop computers, lean clients, web phones, or workstations. Telephones 110 and 120 can be analog or digital and can be separate from or part of computers 105 and 115,
20 respectively. In one implementation, application programs or agents (e.g., software routines that wait in the background and perform an action when a specified event occurs) executing on computers 105 and 115 can monitor analog

and/or digital signals sent to telephones 110 and 120,
respectively.

Computers 105 and 115 are connected to a computer
network 125. Computer network 125 can be an Internet
5 protocol ("IP") network, such as the global Internet or an
intranet. In one implementation, computers 105 and 115 are
connected to the Internet logically independent of the
telephones' PSTN network connections, such as by a xDSL
phone line, a cable modem connection, ISDN connection,
10 Internet accessible LAN connection, or second POTS line.

Telephones 110 and 120 are connected to a communication
network 130, e.g., a voice telephone network such as a
public switched telephone network ("PSTN", or plain old
telephone service network, "POTS") or a private branch
15 exchange ("PBX"). The connections to telephone network 130
can be analog and/or digital, depending upon the nature of
telephones 110 and 120 and any equipment such as PBXs which
might be in the connection path.

Computers 105 and 115 can be used to augment the
20 telephone communications by leveraging their connections to
computer network 125 and telephone network 130. While users
are talking across telephone network 130 using telephones
110 and 120, they can automatically (e.g., by using the

computers to establish a computer network connection) and spontaneously (e.g., without pre-arrangement between the users) access functionality provided by applications running on computers 105 and 115 by utilizing computer network 125.

5 By accessing both the telephone connection and the computer network connection, the users can work together (e.g., collaborate) across both connections.

Users can access spontaneous network collaboration during a telephone connection by sending a computer network address across the communication network 130 which is different than the computer network connection. This can be done, for example, by a touch tone Dual Tone Multi Frequency (DTMF) sequence, a modem sequence or by transmitting the data network address with the caller ID. The computer

10 address across the communication network 130 which is different than the computer network connection. This can be done, for example, by a touch tone Dual Tone Multi Frequency (DTMF) sequence, a modem sequence or by transmitting the data network address with the caller ID. The computer

15 network address information is sent across a different network than the computer network and so is "out-of-band" relative to the computer network. In one implementation, the system used is automatic and done with reduced negotiation time faster than training sequences.

20 Training is an initial connection process a modem receiver uses to synchronize to a remote modem's transmit signal. Training may also occur during a connection usually to correct for extreme disruptions such as line outages or

bursts of line noise. Training is actually the result of many interim tasks a modem performs to make a connection, such as automatic gain control adjustment, receiver timing acquisition, half-duplex equaliser convergence, echo
5 cancellation convergence, full-duplex echo cancellation, equalizer convergence, and more. These tasks all occur during the initial handshake of the connection. During training, no data is transmitted, so from an application perspective it's lost time. A conventional fast train
10 sequence can last about seven seconds.

The recipient uses this computer network address to establish a substantially simultaneous and related connection across computer network 125, e.g., via the Internet. This connection provides users with the ability
15 to spontaneously access computer network connectivity and computer functionality, such as for a graphical link to access network collaboration software, simultaneously with a telephone connection. One example of collaboration software is a synchronized web browser, where one party's navigation
20 of the web drives the navigation of the web of the other party. Another example is video conferencing, where the PSTN's ability to provide a high quality of service complements by video transmitted over the Internet. This

technique provides benefits such as: lowered complexity of using a computer, software applications, and the Internet to enhance phone conversations through automatic connection, voice enabled computer collaboration without audio quality
5 problems associated with Internet telephony, spontaneous connection without requiring a directory service to keep track of dynamic or unknown IP addresses.

Computers 105 and 115 can also be configured with crossbar switches (e.g., N x N switches) to dynamically
10 allocate audio input ports and output ports during a telephone connection, as described below. A user can connect one or more input ports to one or more output ports and change these connections without terminating the telephone connection. The crossbar switches allow users to
15 dynamically set up and tear down connections between input ports and output ports in real-time. This allows a single device to be used for multiple speech interactions, such as telephony over the PSTN, Internet telephony, web-to-phone communications established through a remote web site, and
20 local or remote voice control of a computer. Application programs executing on a computer can monitor audio signals on a connected PSTN line or Internet telephonic connection. The switch can also provide a uniform audio interface for

application vendors independent of devices and connection media.

5 Users can enhance privacy of communications across a telephone connection by using the computer to encrypt audio signals (e.g., electrical signals representing audible sounds) before transmission. Users establish a telephone connection and a computer network connection. A user at telephone 110 sends a secret key across computer network 125. The user then encrypts audio signals using computers 10 105 and sends the encrypted signals across telephone network 130. The recipient decrypts the signal using computer 115. This encryption provides cost-effective crypto-phone capabilities and enhanced security by utilizing, for example, computer processing power, computer security 15 features such as random number generators, private/public key pairs, and hidden execution capabilities.

20 Users can also enhance telephone communications by authenticating the identity of a caller using computer network 125 and telephone network 130, in applications such as commercial transactions. Users establish a telephone connection and a computer network connection. A user at telephone 110 sends a secret key generated by 105 across telephone network 130 using a mechanism such as DTMF to a

user at telephone 120. The user at telephone 120 returns
the secret key across computer network 125. The computer at
telephone 110 verifies that the received secret key is the
same as the secret key originally sent. This verification
5 confirms that telephone 120 is coupled to computer 115. The
users can then use conventional digital certification
techniques to verify the identity of computers 105 and 115.
By verifying the connection between telephone 120 and
computer 115, the user at telephone 110 can attribute to the
10 user at telephone 120 the level of trust provided by the
identification credentials stored on, or transmitted via
computer 115. Mechanisms to ascertain the validity of the
credentials can proceed using the Internet, as if the
transaction were initiated on the computer using the
15 Internet.

The configuration shown in FIG. 1 can also be
implemented in various alternative ways. Computers 105 and
115 can be coupled directly to telephone network 130 via a
PBX, key system, or cellular network. Computers 105 and 115
20 can be individually connected to computer network 125, or
collectively with other computers via a local or wide area
network ("LAN" or "WAN"). Computers 105, 115 and telephones
110, 120 can be connected to computer network 125 and

telephone network 130 through digital subscriber line ("DSL" or "xDSL") connections. An xDSL connection provides two logical signal paths across a signal physical line. Hence, computer 105 and telephone 110 can share a single physical
5 connection to telephone network 130. Computer 105 can access computer network 125 through a PoP connection to the Internet. In addition, more than two computers and telephones can be connected, such as in a conference call.

FIG. 2 is a flowchart 200 showing the operations of
10 spontaneously, e.g., without previous arrangements, establishing an IP connection between computers of user A and user B using the public switched telephone network ("PSTN") and the configuration shown in FIG. 1. Users A and B each establish active connections to the Internet at 205.
15 Upon establishing these connections, the computers for users A and B each receive an IP address if addresses are dynamically assigned. User A calls user B across the PSTN, establishing a telephone connection, 210. An application or agent on computer 105 causes the IP address for user A's
20 computer to be encoded by either the computer 105 or the attached phone 110 in a form that can be sent across the PSTN, 215. This encoding can be using a dual tone multi-frequency ("DTMF") coding. Instead of an IP address, the

application or agent can supply a reference to the IP address of computer 105, such as an entry in a known directory.

5 User A sends the encoded IP address to user B's computer 115 across the PSTN 130, through user B's phone 120, 220. User A can send the IP address in various ways. For example, the IP address can be sent using DTMF signaling over the same channel as the user information (e.g., speech) or digitally encoded and sent along with caller ID through
10 the telephone signaling channel. User A sends the encoded IP address for a computer network connection across the telephone network connection, a separate network from the computer network, so the signaling is "out-of-band signaling." In one implementation, a telephone can include
15 a "SEND" button. When user A presses the SEND button, the telephone requests the IP address from the computer 105 through connection 107. The IP address can be provided in any format. The telephone then transmits the tones in a predetermined format such as hexadecimal encoding, using a
20 mechanism such as DTMF encoding across the PSTN connection to user B's telephone.

An application program or agent executing on user B's computer detects the encoded IP address as the address.

This is received at user B's telephone at 225. To facilitate this detection, the encoding can include a pre-defined flag to indicate an IP address. The agent decodes the IP address, 230. The agent establishes communications, 5 such as by sending a network connection request, across the Internet using the decoded IP address for user A's computer to connect to user A's computer, 235.

Once the IP connection has been established, users A and B can continue to converse across the PSTN connection as 10 well as run applications which utilize network connections. Examples of such applications include collaboration software, joint web browsing software, video, and network games.

Various alternative implementations are possible. For 15 example, user A's telephone can send the encoded IP address for user A's computer as header information when the telephone connection is initially established, similar to information identifying user A's telephone (e.g., "caller ID"). When multiple users are connected across the PSTN, 20 such as in a conference call, user A can cause the IP address for user A's computer to be sent to all or some of the users. These users can then select whether to establish an IP connection. User A can initiate the transmission of

the IP address by executing an application which employs an IP connection, such as network collaboration software.

Operations performed by the agent on user B's computer can alternatively be performed by an application program under
5 the control of user B. Once the IP connection is established, the computers can open an Internet telephony connection and cause the PSTN connection to end.

FIG. 3A is a block diagram 300 of a second embodiment. An audio source 305 is coupled to an audio crossbar switch
10 310. Audio source 305 supplies an audio signal to crossbar switch 310. Audio source 305 can be a telephone or some other audio source, such as a microphone, computer sound system, or a connection to a network. Crossbar switch 310 has output ports respectively coupled to a telephone network
15 315, such as the PSTN, a computer network 320, such as the Internet, and a computer 325. Output ports of crossbar switch 310 can be coupled to other devices as well, such as audio speakers or recording equipment. A control element 330 supplies control signals to crossbar switch 310 to cause
20 crossbar switch 310 to output the audio signal from one or more of the output ports of crossbar switch 310.

In FIG. 3A, crossbar switch 310 is shown with one input port and three output ports. However, crossbar switch 310

can have more or less input ports and output ports. Control element 330 can cause crossbar switch 310 to connect any combination of available input ports to any combination of available output ports. In addition, input ports and output
5 ports can support two-way signaling, so that, for example, crossbar switch 310 can send signals to and receive signals from computer 325. Alternatively, each input port or output port can provide a pair of couplings, one for input and one for output.

10 FIG. 3B is a block diagram 350 showing a crossbar switch 310 coupled to a computer, such as computer 105 in FIG. 1. Telephone 110 is coupled to an input port of crossbar switch 310. Computer 105, and telephone network 130 are coupled to output ports of crossbar switch 310.
15 Computer 105 is also coupled to control element 330. Crossbar switch 310 can be implemented as an internal component of computer 105 or telephone 110.

A user at telephone 110 can route audio signals from telephone 110 through crossbar switch 310 to any one or more
20 of its output ports: telephone network 130, computer 105, and computer network 125 through computer 105. The user can command crossbar switch 310 to change the routing dynamically, without terminating a telephone connection.

5 Crossbar switch 310 can preserve the telephone connection by
establishing a second network connection before terminating
the original network connection. For example, in one
implementation, when the user has established a telephone
connection across telephone network 130 and commands
crossbar switch 310 to switch to a telephone connection
across computer network 125, after the computer network
connection has been established as described above, crossbar
switch 310 connects the ports corresponding to telephone 110
10 and computer network 130 while maintaining the connection
between the ports corresponding to telephone 110 and
telephone network 125. After connecting the ports for
telephone 110 and computer network 125, crossbar switch 310
ends the connection between the ports for telephone 110 and
15 telephone network 130. Crossbar switch 310 can also route
information from computer 105 and telephone network 130 to
telephone 110, using the configurable two-way nature of the
input ports and output ports.

20 In one example of operation, crossbar switch 310 can be
used to support encrypting a conversation being sent across
telephone network 130. A user speaks into telephone 110 and
crossbar switch 310 sends the audio signal to telephone
network 130. The user then activates encryption so that

computer 105 adjusts control element 330. When the user speaks, crossbar switch 310 routes the audio signal to computer 105. Computer 105 encrypts the audio signal and returns the encrypted signal to crossbar switch 310.

5 Crossbar switch 310 sends the encrypted signal to telephone network 130. Alternatively, the encrypted signal can be sent across computer network 125. Encryption is also described below.

666040-5063260
10 In another example, crossbar switch 310 provides a transparent real-time shift from a telephone network connection to a computer network connection. A user at telephone 110 establishes a connection across telephone network 130. Crossbar switch 310 routes audio signals from telephone 110 to telephone network 130. The user also
15 establishes a computer network connection, such as by the process described above for spontaneous IP connections. When the user activates an IP telephony application program on computer 105, computer 105 causes crossbar switch 310 to route the audio signals from telephone 110 to computer 105,
20 without interrupting the telephone conversation. This operation can occur simultaneously with a switching of the voice stream on the other side of the network.

FIG. 4 is a flowchart 400 showing the process of encrypting an audio signal sent over a telephone connection, such as the PSTN, using a computer network connection, such as an IP connection, to facilitate the secure exchange of
5 keys. Users A and B have access to computers and telephones configured as shown in FIG. 1. In one implementation, the computers include crossbar switches, as described above. Users A and B each establish active connections to the Internet, 405. As part of establishing these connections,
10 the computers for users A and B each receive an IP address. User A calls user B across the PSTN, establishing a telephone connection, 410. Users A and B establish a peer to peer IP connection, 415, such as by the process described above and shown in FIG. 2.

15 User A then sends a secret key to user B across the IP connection, 420. The secret key is a cryptographic key for encrypting and decrypting information, such as a key for use with the data encryption standard ("DES") cryptography method. In one implementation, the secret key is generated
20 by security hardware built into user A's computer. User A can send the secret key to user B using a digital envelope constructed with a public key cryptography method, such as the Rivest-Shamir-Adleman ("RSA") method. Thus, user A

encrypts the secret key with user B's public key. User B decrypts the secret key using user B's private key. The cross bar switch is configured such that audio signals from the telephone is routed from the telephone to the computer.

5 Computer A encrypts the audio signal to be sent to user B using the secret key, 425. The encryption is transparent to user A. User A activates a security application program or agent and that agent encrypts audio signals received from user A's telephone. Computer A sends
10 the encrypted signal to user B across the PSTN, 430. Computer B decrypts the encrypted signal using the secret key, 435. This decryption is also transparent to user B. User B activates a security application program or agent and that agent decrypts encrypted signals received at user B's
15 telephone. An identical process can encrypt audio signals from User B to User A. Thus, once the secret key has been transferred across the IP connection, the users can converse across the PSTN connection while the computers encrypt and decrypt the users' audio signals.

20 FIG. 5 is a flowchart 500 showing authenticating a caller during a telephone connection across a telephone network, such as the PSTN, using a computer network connection, such as an IP connection. Users A and B have

access to computers and telephones configured as shown in
FIG. 1. Users A and B each establish active connections to
the Internet at 505. As part of establishing these
connections, the computers for users A and B each receive an
5 IP address. User B calls user A across the PSTN,
establishing a telephone connection, 510. Users A and B
establish an IP connection, 515, such as by the process
described above and shown in FIG. 2.

To authenticate user B, user A verifies that the
10 telephone that user B is using at the remote end of the
telephone connection is coupled to the computer at the
remote end of the IP connection, 520. User A verifies this
telephone-computer connection by sending a secret key signal
across the PSTN and receiving the same signal back from user
15 B across the IP connection. One example of this
verification is described below with respect to FIG. 6.
Once User A verifies that user B's computer is the computer
that user B asserts, conventional digital certification
across the IP connection can be deployed to verify the
20 validity of user B's digital credentials, 525. If a device
such as a smart card reader or a biometric identification
device such as a fingerprint reader or retina scanner is

configured on computer B, these can also be used as part of the identification validation process.

FIG. 6 is a flowchart 600 of verifying the telephone-computer connection between user B's telephone and computer.

5 User A generates a secret key including a random number using user A's computer, 605. The random number can be generated by hardware. User A sends the random number to user B across the PSTN, 610, using a mechanism such as Hex encoding and DTMF signaling. User B returns the random
10 number across the IP connection, 615.

User A compares the random number received over the Internet with the original random number sent over the PSTN, 620. If the Internet random number matches the original random number sent to user B, user A has verified that the
15 telephone and computer of user B are coupled. This verification provides an additional level of security in transactions occurring across the PSTN. User A can verify that the caller has access to user B's computer using conventional digital certification. Using the technique
20 described above, user A can also verify that the caller is using the telephone coupled to user B's computer. Authentication techniques continue to advance in fields such as biometrics. The ability to authenticate using a

telephone connection provides a corresponding improvement in security.

INS DIS
The technique of the present disclosure may be implemented in hardware or software, or a combination of
5 both. Portions of the technique can be implemented by means of a computer program executing on one or more programmable systems each comprising at least one processor, a data storage system (including volatile and non-volatile memory and/or storage elements), at least one input device,
10 and at least one output device. Program code is applied to input data to perform the functions described herein and generate output information. The output information is applied to one or more output devices, in known fashion. The processor may comprise, for example, a general purpose
15 processor or a digital signal processor (DSP).

Each program can be implemented in a high level procedural or object oriented programming language to communicate with a computer system although the invention is not limited in this respect. However, the programs can be
20 implemented in assembly or machine language, if desired. In any case, the language may be a compiled or interpreted language.

Each such computer program can be stored on a storage media or device (e.g., ROM or magnetic diskette) readable by a general or special purpose programmable computer, for configuring and operating the computer when the storage
5 media or device is read by the computer to perform the procedures described herein. The inventive system may also be considered to be implemented as a computer-readable storage medium, configured with a computer program, where the storage medium so configured causes a computer to
10 operate in a specific and predefined manner to perform the functions described herein.

Various implementations have been described. However, these implementations are examples and are not limiting. For example, the order of operations of the processes
15 described is illustrative and alternative orders are possible. Both computers need not be connected to the computer network when the telephone connection is initially established. The "user" on one side of the connection can be automated, such as when a user calls a computer-
20 controlled interactive voice response system, allowing a user to enhance interaction with a remote computer with graphical content. The encoding of an IP address can be performed within the telephone. Numerous security,

cryptography, and authentication techniques, implemented in hardware and software, are well known and can be used. The voice network can be any voice system, including cellular or the like. This technique also applies to protocols other
5 than IP. Addresses transmitted may or may not include associated application identifiers such as ports. The addresses transmitted might not be for the computer engaged in the transaction, but for a proxy on the network associated with the computer. The random number used for
10 verifying the connection between a computer and a telephone can be encrypted. The technique can be used to verify a connection between devices other than computers and telephones.